CYBER RISKS & LIABILITIES_
NEWSLETTER

April / May 2014

IN THIS ISSUE

The ICO's 5 'Bring Your Own Device' Recommendations

Personal devices are everywhere. A December 2013 survey found that 60 per cent of the UK population owns a smart phone, and 20 per cent owns a tablet. Personal devices permeate every aspect of people's lives—communication, shopping, banking and even jobs.

Due to the inextricable link between people and their devices, it makes sense that employers would let their employees use personal devices at work, a trend known as 'bring your own device' (BYOD). Using personal devices for work while on the job can increase efficiency, flexibility and employee morale. Employees can have access to more information, making them more efficient; they can be mobile but reachable via their devices; and they can feel happier about a job which lets them stay connected to the device that connects them to their family and friends.

But the BYOD trend is not without its risks. If an employee uses his or her personal device to process work data but then loses that device, the organisation's data is now compromised. You can have it both ways—allowing your employees to use their own devices for work while also safeguarding your organisation's data—by following these recommendations for BYOD policies from the Information Commissioner's Office (ICO).

1. **Ensure devices are secure.** The first step in establishing a safe, low-risk BYOD policy is making sure the devices themselves are secure. To prevent unauthorised access, lock devices with a strong password, separate work data from personal data and use encryption to securely store data.

2. **Secure data transfers between personal devices and organisational systems.** Data is vulnerable when transferring from one device to another. Only transfer data via a secure channel. Be wary of untrusted connections such as public Wi-Fi in a coffee shop.

3. **Retain control of all devices.** If an employee's device is lost or stolen, ensure you can prevent unauthorised access of any work-related data. Register devices with a facility that remotely locates and wipes devices of data if they are lost or stolen.

4. **Have an end of contract policy.** Be prepared to retrieve work-related information if employees leave the company or replace their devices. Learn how to change passwords and revoke access to your organisation's systems.

5. **Provide a clear acceptable use policy.** Your management and employees should understand their responsibilities. Clearly state which types of personal information may be processed on personal devices.

Rely on Crendon Insurance Brokers Ltd for examples of existing BYOD policies and for help with writing one perfectly suited to your organisation.

Crendon Insurance Brokers

Guard Your Data From External and Internal Threats

A data theft in March 2014 from UK supermarket Morrisons highlights the need to guard against internal security threats in addition to threats from external sources. A Morrisons employee was arrested for stealing and publishing the bank details of about 100,000 Morrison employees online.

The data theft affected all levels of the organisation, according to the supermarket. Specific motivations for the theft remain unclear, although the theft quickly sent Morrisons' shares plunging down 12 per cent once it became public knowledge.

This theft calls attention to the swift backlash that accompanies data thefts and the very real threat posed by internal data thieves. Being part of an organisation does not stop people from stealing that organisation's data.

How are businesses supposed to prevent external and internal threats to data security? Consider some of the following tips to keep your data secure from prying eyes—both inside and outside your organisation.

- Divide data maintenance duties among a large pool of employees to decrease the likelihood of fraud.
- Perform a pre-employment screening on all potential employees.
- Educate employees about your company's policies on employee theft.
- Recognise high-risk departments like accounting, purchasing and upper management as potential sources of fraud.
- Conduct random audits to set up and maintain effective internal financial controls.
- Do not get complacent—remember that any employee can commit fraud.

British Pregnancy Advice Service fined

The British Pregnancy Advice Service (BPAS) was fined £200,000 after its lax cyber security and weak website code allowed a malicious hacker to access the personal information of thousands of people who had called the service for advice on pregnancy, birth control and other sexual issues. An investigation by the ICO discovered the charity did not even realise that its website stored the names, addresses, dates of birth and telephone numbers of callers. In addition to failing to secure personal information, the BPAS also breached the Data Protection Act by retaining call information five years longer than necessary. Although the BPAS was woefully ignorant of its violations, ignorance is not a valid excuse for avoiding fines.

Department of Justice Northern Ireland fined

In an embarrassing oversight, the Department of Justice Northern Ireland (DoJ NI) was fined £185,000 for inadvertently releasing sensitive personal information relating to victims of a terrorist incident. The DoJ NI sold a filing cabinet to a member of the public in May 2012, but neglected to inspect the cabinet's interior, which contained papers dating from the 1970s to 2005, before selling it. The buyer, on finding the documents, realised they were important and quickly contacted the Police Service Northern Ireland to return them.

Avoid fines by registering your company with the ICO

A green energy company based in Cardiff was prosecuted by the ICO after failing to disclose that it handled customers' personal data. The company's director was fined £270 and ordered to pay a £27 victim surcharge and £300 in prosecution costs. The company was fined the same amounts. Under the Data Protection Act, companies must register with the ICO if they handle customers' personal data. That way the ICO can ensure companies deal with sensitive data securely and compliantly. Generally, registration involves paying an annual notification fee of £35 and providing information on the types of personal data the company processes. Weigh your options—would you rather pay £35 now or £600 later?

CYBERRISKS&LIABILITIES_
NEWSLETTER

Crendon Insurance Brokers Ltd
11 Greenfield Crescent
Birmingham, West Midlands, B15 3AU
0121 454 5100
www.crendoninsurance.co.uk